Amendments to the Claims

Claim 1 (previously presented): A computer program product embodied on one or more computer-readable media, for establishing a secure connection between a client application and a server application using pre-existing message types, said computer program product comprising:

computer-readable program code means for piggy-backing a request for a message encoding scheme proposal onto a first message sent from said client application to said server application, wherein said first message uses a first pre-existing message type;

computer-readable program code means for piggy-backing a first portion of security information onto a second message sent from said server application to said client application, wherein said second message uses a second pre-existing message type and wherein said first portion comprises a response to said request for a message encoding scheme;

computer-readable program code means for piggy-backing a second portion of security information onto a third message sent from said client application to said server application, wherein said third message uses said first pre-existing message type; and

computer-readable program code means for piggy-backing a third portion of security information onto a fourth message sent from said server application to said client application, wherein said fourth message uses a third pre-existing message type.

Claim 2 (previously presented): The computer program product according to Claim 1, wherein said first pre-existing message type is a HyperText Transfer Protocol (HTTP) GET request message, said second pre-existing message type is an HTTP REDIRECT message, and said third pre-existing message type is a response to said HTTP GET request message.

Claim 3 (previously presented): The computer program product according to Claim 1, wherein said first pre-existing message type is a HyperText Transfer Protocol (HTTP) POST request message, said second pre-existing message type is an HTTP REDIRECT message, and said third pre-existing message type is a response to said HTTP POST request message.

Claim 4 (previously presented): The computer program product according to Claim 1, wherein said first pre-existing message type is a Wireless Session Protocol (WSP) GET request message, said second pre-existing message type is a WSP REDIRECT message, and said third pre-existing message type is a response to said WSP GET request message.

Claim 5 (previously presented): The computer program product according to Claim 1, wherein said first pre-existing message type is a Wireless Session Protocol (WSP) POST request message, said second pre-existing message type is a WSP REDIRECT message, and said third pre-existing message type is a response to said WSP POST request message.

Claim 6 (original): The computer program product according to Claim 1, wherein:

said first message requests a secure page from said server application, wherein said secure page request further comprises an identifier of said secure page;

said second message sends a redirection message from said server application to said client application, wherein said redirection message comprises a redirected identifier of said secure page;

said third message sends a subsequent request for said secure page from said server application in response to said redirection message, wherein said subsequent request further comprises said redirected identifier of said secure page; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

Claim 7 (original): The computer program product according to Claim 6, wherein:

said first portion further comprises a security certificate of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

Claim 8 (original): The computer program product according to Claim 6, wherein:

said first portion further comprises an identification of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

Claim 9 (original): The computer program product according to Claim 7 or Claim 8, wherein said request for a message encoding scheme further comprises a keyword indicating said request.

Claim 10 (original): The computer program product according to Claim 9, wherein said set of information comprises: zero or more parameters required for said secure page request; an identification of said client application; a client nonce; and optionally including a timestamp.

Claim 11 (previously presented): The computer program product according to Claim 6, wherein said redirected identifier of said secure page is identical to said identifier of said secure page.

Claim 12 (original): The computer program product according to Claim 1, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page;

said second message sends an authentication message from said server application to said client application;

said third message sends a subsequent request for said secure page from said server application in response to said authentication message; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

Claim 13 (original): The computer program product according to Claim 12, wherein said authentication message comprises a redirected identifier of said secure page, and wherein said subsequent request further comprises said redirected identifier of said secure page.

Claim 14 (previously presented): A system for establishing a secure connection between a client application and a server application using pre-existing message types, said system comprising:

means for piggy-backing a request for a message encoding scheme proposal onto a first message sent from said client application to said server application, wherein said first message uses a first pre-existing message type;

means for piggy-backing a first portion of security information onto a second message sent from said server application to said client application, wherein said second message uses a second pre-existing message type and wherein said first portion comprises a response to said request for a message encoding scheme;

means for piggy-backing a second portion of security information onto a third message sent from said client application to said server application, wherein said third message uses said first pre-existing message type; and

means for piggy-backing a third portion of security information onto a fourth message sent from said server application to said client application, wherein said fourth message uses a third pre-existing message type.

Claim 15 (previously presented): The system according to Claim 14, wherein said first pre-existing message type is a HyperText Transfer Protocol (HTTP) GET request message, said second pre-existing message type is an HTTP www-Authenticate message header, and said third pre-existing message type is a response to said HTTP GET request message.

Claim 16 (previously presented): The system according to Claim 14, wherein said first pre-existing message type is a HyperText Transfer Protocol (HTTP) POST request message, said second pre-existing message type is an HTTP www-Authenticate message header, and said third pre-existing message type is a response to said HTTP POST request message.

Claim 17 (previously presented): The system according to Claim 14, wherein said first pre-existing message type is a Wireless Session Protocol (WSP) GET request message, said second pre-existing message type is a WSP www-Authenticate message header, and said third pre-existing message type is a response to said WSP GET request message.

Claim 18 (previously presented): The system according to Claim 14, wherein said first pre-existing message type is a Wireless Session Protocol (WSP) POST request message, said second pre-existing message type is a WSP www-Authenticate message header, and said third pre-existing message type is a response to said WSP POST request message.

Claim 19 (original): The system according to Claim 14, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page;

said second message sends an authentication message from said server application to said client application;

said third message sends a subsequent request for said secure page from said server application in response to said authentication message; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

Claim 20 (original): The system according to Claim 19, wherein said authentication message comprises a redirected identifier of said secure page, and wherein said subsequent request further comprises said redirected identifier of said secure page.

Claim 21 (original): The system according to Claim 19 or Claim 20, wherein:

said first portion further comprises a security certificate of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

Claim 22 (original): The system according to Claim 19 or Claim 20, wherein:

said first portion further comprises an identification of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

Claim 23 (original): The system according to Claim 20, wherein said request for a message encoding scheme further comprises a keyword indicating said request.

Claim 24 (original): The system according to Claim 23, wherein said set of information comprises: zero or more parameters required for said secure page request; an identification of said client application; a client nonce; and optionally including a timestamp.

Claim 25 (original): The system according to Claim 22, wherein said request for a message encoding scheme further comprises a keyword indicating said request and wherein said set of information comprises: zero or more parameters required for said secure page request; an identification of said client application; a client nonce; and optionally including a timestamp.

Claim 26 (previously presented): The system according to Claim 20, wherein said redirected identifier of said secure page is identical to said identifier of said secure page.

Claim 27 (original): The system according to Claim 14, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page;

said second message sends a redirection message from said server application to said client application, wherein said redirection message comprises a redirected identifier of said secure page;

said third message sends a subsequent request for said secure page from said server application in response to said redirection message, wherein said subsequent request further comprises said redirected identifier of said secure page; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

Claim 28 (previously presented): A method for establishing a secure connection between a client application and a server application using pre-existing message types, said method comprising the steps of:

piggy-backing a request for a message encoding scheme proposal onto a first message sent from said client application to said server application, wherein said first message uses a first pre-existing message type;

piggy-backing a first portion of security information onto a second message sent from said server application to said client application, wherein said second message uses a second pre-existing message type and wherein said first portion comprises a response to said request for a message encoding scheme;

piggy-backing a second portion of security information onto a third message sent from said client application to said server application, wherein said third message uses said first pre-existing message type; and

piggy-backing a third portion of security information onto a fourth message sent from said server application to said client application, wherein said fourth message uses a third pre-existing message type.

Claim 29 (previously presented): The method according to Claim 28, wherein said first pre-existing message type is a HyperText Transfer Protocol (HTTP) GET request message, said second pre-existing message type is an HTTP www-Authenticate message header, and said third pre-existing message type is a response to said HTTP GET request message.

Claim 30 (previously presented): The method according to Claim 28, wherein said first pre-existing message type is a HyperText Transfer Protocol (HTTP) POST request message, said second pre-existing message type is an HTTP www-Authenticate message header, and said third pre-existing message type is a response to said HTTP POST request message.

Claim 31 (previously presented): The method according to Claim 28, wherein said first pre-existing message type is a Wireless Session Protocol (WSP) GET request message, said second pre-existing message type is a WSP www-Authenticate message header, and said third pre-existing message type is a response to said WSP GET request message.

Claim 32 (previously presented): The method according to Claim 28, wherein said first pre-existing message type is a Wireless Session Protocol (WSP) POST request message, said second pre-existing message type is a WSP www-Authenticate message header, and said third pre-existing message type is a response to said WSP POST request message.

Claim 33 (original): The method according to Claim 28, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page;

said second message sends an authentication message from said server application to said client application;

said third message sends a subsequent request for said secure page from said server application in response to said authentication message; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

Claim 34 (original): The method according to Claim 33, wherein said authentication message comprises a redirected identifier of said secure page, and wherein said subsequent request further comprises said redirected identifier of said secure page.

Claim 35 (original): The method according to Claim 33 or Claim 34, wherein:

said first portion further comprises a security certificate of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

Claim 36 (original): The method according to Claim 33 or Claim 34, wherein:

said first portion further comprises an identification of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

Claim 37 (original): The method according to Claim 34, wherein said request for a message encoding scheme further comprises a keyword indicating said request.

Claim 38 (original): The method according to Claim 37, wherein said set of information comprises: zero or more parameters required for said secure page request; an identification of said client application; a client nonce; and optionally including a timestamp.

Claim 39 (original): The method according to Claim 36, wherein said request for a message encoding scheme further comprises a keyword indicating said request and wherein said set of information comprises: zero or more parameters required for said secure page request; an identification of said client application; a client nonce; and optionally including a timestamp.

Claim 40 (previously presented): The method according to Claim 34, wherein said redirected identifier of said secure page is identical to said identifier of said secure page.

Claim 41 (original): The method according to Claim 28, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page;

said second message sends a redirection message from said server application to said client application, wherein said redirection message comprises a redirected identifier of said secure page;

said third message sends a subsequent request for said secure page from said server application in response to said redirection message, wherein said subsequent request further comprises said redirected identifier of said secure page; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

Claim 42 (currently amended): A method for establishing a secure connection between a client application and a server application using pre-existing message types, said method comprising the steps of:

piggy-backing a request for said server application to select a message encoding scheme onto a ~~first message~~ content request sent from said client application to said server application, wherein said ~~first message~~ content request uses a first pre-existing message type to request content from, or deliver content to, said server application;

selecting, by said server application without using information from, or pre-arranged with, said client application, a message encoding scheme, responsive to said content request;

using, by said server application, said selected message encoding scheme to encrypt security-sensitive content for sending to said client application, responsive to said content request; and

piggy-backing ~~a first portion of~~ security information onto ~~a second message~~ content response sent from said server application to said client application, wherein said ~~second message~~ content response uses a second pre-existing message type and responds to said ~~first message~~ content request by sending said encrypted security-sensitive content, wherein said piggy-backed security information ~~security-sensitive content is encrypted using a server-application-selected message encoding scheme that is thereby proposed to said client application and said first portion~~ enables said client application to determine said selected message encoding scheme, such that said client can then decrypt said security-sensitive content.

Claim 43 (previously presented): The method according to Claim 42, wherein said first pre-existing message type is a HyperText Transfer Protocol (HTTP) GET request message and said second pre-existing message type is a response to said HTTP GET request message.

Claim 44 (previously presented): The method according to Claim 42, wherein said first pre-existing message type is a HyperText Transfer Protocol (HTTP) POST request message and said second pre-existing message type is a response to said HTTP POST request message.

Claim 45 (previously presented): The method according to Claim 42, wherein said first pre-existing message type is a Wireless Session Protocol (WSP) GET request message and said second pre-existing message type is a response to said WSP GET request message.

Claim 46 (previously presented): The method according to Claim 42, wherein said first pre-existing message type is a Wireless Session Protocol (WSP) POST request message and said second pre-existing message type is a response to said WSP POST request message.

Claim 47 (currently amended): The method according to Claim 42, wherein:

said ~~first message~~ content request requests said security-sensitive content from said server application, wherein said request further comprises an identifier with which said security-sensitive content can be located;

said security-sensitive content in said ~~second message~~ content response is encrypted using a session key generated by said server application; and

said ~~first portion~~ security information secures said session key while enabling said client application to securely recover said session key.

Claim 48 (currently amended): The method according to Claim 47, wherein:

said request to select a message encoding scheme further comprises an identifier of said client application, a nonce of said client application, and optionally includes a timestamp; and

said ~~first portion~~ security information is secured using a public key of said client ~~server~~ application.

Claim 49 (currently amended): The method according to Claim [[48]] 47, wherein said ~~first~~

~~portion~~ security information further comprises:

a nonce of said server application, encrypted using a public key of said client application; and

a security certificate of said server application.

Claim 50 (currently amended): The method according to Claim 48 or Claim 49, wherein ~~first message~~ said content request further comprises zero or more parameters required for said server application to use when preparing said security-sensitive content.

Claim 51 (currently amended): A system for establishing a secure connection between a client application and a server application using pre-existing message types, said system comprising:

means for piggy-backing a request for said server application to select a message encoding scheme onto ~~a first message~~ content request sent from said client application to said server application, wherein said ~~first message~~ content request uses a first pre-existing message type to request content from, or deliver content to, said server application;

means for selecting, by said server application without using information from, or pre-arranged with, said client application, a message encoding scheme, responsive to said content request;

means for using, by said server application, said selected message encoding scheme to encrypt security-sensitive content for sending to said client application, responsive to said content request; and

means for piggy-backing ~~a first portion of~~ security information onto a content response

~~second message~~ sent from said server application to said client application, wherein said content response ~~second message~~ uses a second pre-existing message type and responds to said content request ~~first message~~ by sending said encrypted security-sensitive content, wherein said piggy-backed security information ~~security-sensitive content is encrypted using a server-application-selected message encoding scheme that is thereby proposed to said client application and said first portion~~ enables said client application to determine said selected message encoding scheme, such that said client application can then decrypt said security-sensitive content.

Claim 52 (previously presented): The system according to Claim 51, wherein said first pre-existing message type is a HyperText Transfer Protocol (HTTP) GET request message and said second pre-existing message type is a response to said HTTP GET request message.

Claim 53 (previously presented): The system according to Claim 51, wherein said first pre-existing message type is a Wireless Session Protocol (WSP) GET request message and said second pre-existing message type is a response to said WSP GET request message.

Claim 54 (currently amended): The system according to Claim 51, wherein:

said ~~first message~~ content request requests said security-sensitive content from said server application, wherein said request further comprises an identifier with which said security-sensitive content can be located;

said security-sensitive content in said ~~second message~~ content response is encrypted using a session key generated by said server application; and said ~~first portion~~ security information secures said session key while enabling said client application to securely recover said session key.

Claim 55 (currently amended): The system according to Claim 54, wherein:

said request to select a message encoding scheme further comprises an identifier of said client application, a nonce of said client application, and optionally includes a timestamp; and

said ~~first portion~~ security information is secured using a public key of said ~~server~~ client application.

Claim 56 (currently amended): The system according to Claim [[55]] 54, wherein said ~~first portion~~ security information further comprises:

a nonce of said server application, encrypted using a public key of said client application; and

a security certificate of said server application.

Claim 57 (currently amended): The system according to Claim 55 or Claim 56, wherein ~~first message~~ said content request further comprises zero or more parameters required for said server application to use when preparing said security-sensitive content.

Claim 58 (currently amended): A computer program product embodied on one or more computer-readable media, for establishing a secure connection between a client application and a server application using pre-existing message types, said computer program product comprising:

computer-readable program code means for piggy-backing a request for said server application to select a message encoding scheme onto a content request ~~first message~~ sent from said client application to said server application, wherein said content request ~~first message~~ uses a first pre-existing message type to request content from, or deliver content to, said server application;

computer-readable program code means for selecting, by said server application without using information from, or pre-arranged with, said client application, a message encoding scheme, responsive to said content request;

computer-readable program code means for using, by said server application, said selected message encoding scheme to encrypt security-sensitive content for sending to said client application, responsive to said content request; and

computer-readable program code means for piggy-backing ~~a first portion of~~ security information onto a content response ~~second message~~ sent from said server application to said client application, wherein said content response ~~second message~~ uses a second pre-existing message type and responds to said ~~first message~~ content request by sending said encrypted security-sensitive content, wherein said piggy-backed security information ~~security-sensitive content is encrypted using a server-application-selected message encoding scheme that is thereby proposed to said client application and said first portion~~ enables said client application to determine said selected message encoding scheme, such that said client application can then decrypt said security-sensitive content.

Claim 59 (previously presented): The computer program product according to Claim 58, wherein said first pre-existing message type is a HyperText Transfer Protocol (HTTP) GET request message and said second pre-existing message type is a response to said HTTP GET request message.

Claim 60 (previously presented): The computer program product according to Claim 58, wherein said first pre-existing message type is a Wireless Session Protocol (WSP) GET request message and said second pre-existing message type is a response to said WSP GET request message.

Claim 61 (currently amended): The computer program product according to Claim 58, wherein:

said ~~first message~~ content request requests said security-sensitive content from said server application, wherein said request further comprises an identifier with which said security-sensitive content can be located;

said security-sensitive content in said ~~second message~~ content response is encrypted using a session key generated by said server application; and

said ~~first portion~~ security information secures said session key while enabling said client application to securely recover said session key.

Claim 62 (currently amended): The computer program product according to Claim 61, wherein:

said request to select a message encoding scheme further comprises an identifier of said client application, a nonce of said client application, and optionally includes a timestamp; and

said ~~first portion~~ security information is secured using a public key of said ~~server~~ client application.

Claim 63 (currently amended): The computer program product according to Claim [[62]] 61, wherein said ~~first portion~~ security information further comprises:

a nonce of said server application, encrypted using a public key of said client application; and

a security certificate of said server application.

Claim 64 (currently amended): The computer program product according to Claim 62 or Claim 63, wherein ~~first message~~ said content request further comprises zero or more parameters required for said server application to use when preparing said security-sensitive content.

Claim 65 (currently amended): A method for securely establishing a connection between a client application and a server application, further comprising steps of:

sending, from the client application to the server application, a first message that uses a first pre-existing message type, wherein the first message requests information from the server application and includes a parameter portion, the parameter portion containing zero or more parameters that may be used by the server application in creating the requested information;

selecting, by the server application responsive to receiving the first message, a message encoding scheme without using information from, or pre-arranged with, the client application;

using, by the server application, the selected message encoding scheme to encrypt the requested information that responds to the first message, the requested information created using zero or more of the zero or more parameters; and sending, from the server application to the client application, a second message, responsive to receiving the first message, wherein:

the second message uses a second pre-existing message type;

the second message contains the encrypted requested information; and

the second message has security information piggy-backed thereon, the piggy-backed security information enabling the client application to determine the selected message encoding scheme, such that the client application can then decrypt the encrypted requested information ~~, which has been created using zero or more of the zero or more parameters and which has been encrypted using a session key;~~

~~the session key has been created using a server nonce; and~~

~~the second message further contains the server nonce, encrypted using a public key of the client application.~~

Claim 66 (currently amended): The method according to Claim 65, wherein a client-provided ~~client~~ nonce is ~~also used when creating the session key, and wherein the client nonce is~~ transmitted on the first message and is used with a server-provided nonce to create a session key for input to the selected message encoding scheme in the using step.

Claim 67 (previously presented): A method for securely establishing a connection between a client application and a server application, further comprising steps of:

sending, from the client application to the server application, a first message that uses a first pre-existing message type, wherein the first message requests information from the server application and signals the server application to propose an encoding scheme to be used for securely establishing the connection;

sending, from the server application to the client application, a second message in response to the first message, wherein the second message uses a second pre-existing message type and requests the client application to re-send the information request from the first message, and wherein the second message also transmits a description of the encoding scheme proposed by the server application;

sending, from the client application to the server application, a third message in response to the second message, wherein the third message uses the first pre-existing message type and re-sends the information request from the first message, along with zero or more parameters to be used by the server application in creating the requested information and first security information for use by the server application in securely establishing the connection, according to the described encoding scheme; and

sending, from the server application to the client application, a fourth message in response to the third message, wherein the fourth message uses a third pre-existing message type and contains the requested information, which has been encrypted using a session key created using the first security information as an input, and wherein the fourth message further comprises second security information which was also used as an input when creating the session key, the second security information encrypted such that it can be decrypted only by the client application.

Claim 68 (previously presented): The method according to Claim 67, wherein the parameters are encrypted using a public key of the server, according to the described encoding scheme.

Claim 69 (previously presented): The method according to Claim 67, wherein the first security information comprises a client nonce and the second security information comprises a server nonce.

Claim 70 (currently amended): A system for securely establishing a connection between a client application and a server application, comprising:

means for sending, from the client application to the server application, a first message that uses a first pre-existing message type, wherein the first message requests information from the server application and includes a parameter portion, the parameter portion containing zero or more parameters that may be used by the server application in creating the requested information;

means for selecting, by the server application responsive to receiving the first message, a message encoding scheme without using information from, or pre-arranged with, the client application;

means for using, by the server application, the selected message encoding scheme to encrypt the requested information that responds to the first message, the requested information created using zero or more of the zero or more parameters; and

means for sending, from the server application to the client application, a second message, responsive to receiving the first message, wherein:

the second message uses a second pre-existing message type;

the second message contains the encrypted requested information; and

the second message has security information piggy-backed thereon, the piggy-backed security information enabling the client application to determine the selected message encoding scheme, such that the client application can then decrypt the encrypted requested information ~~, which has been created using zero or more of the zero or more parameters and which has been encrypted using a session key;~~

~~the session key has been created using a server nonce; and~~

~~the second message further contains the server nonce, encrypted using a public key of the client application.~~

Claim 71 (currently amended): The system according to Claim 70, wherein a client-provided ~~client~~ nonce is ~~also used when creating the session key, and wherein the client nonce is~~ transmitted on the first message and is used with a server-provided nonce to create a session key for input to the selected message encoding scheme in the means for using.

Claim 72 (previously presented): A system for securely establishing a connection between a client application and a server application, comprising:

means for sending, from the client application to the server application, a first message that uses a first pre-existing message type, wherein the first message requests information from the server application and signals the server application to propose an encoding scheme to be used for securely establishing the connection;

means for sending, from the server application to the client application, a second message in response to the first message, wherein the second message uses a second pre-existing message type and requests the client application to re-send the information request from the first message, and wherein the second message also transmits a description of the encoding scheme proposed by the server application;

means for sending, from the client application to the server application, a third message in response to the second message, wherein the third message uses the first pre-existing message type and re-sends the information request from the first message, along with zero or more parameters to be used by the server application in creating the requested information and first security information for use by the server application in securely establishing the connection, according to the described encoding scheme; and

means for sending, from the server application to the client application, a fourth message in response to the third message, wherein the fourth message uses a third pre-existing message type and contains the requested information, which has been encrypted using a session key created using the first security information as an input, and wherein the fourth message further comprises second security information which was also used as an input when creating the session key, the second security information encrypted such that it can be decrypted only by the client application.

Claim 73 (previously presented): The system according to Claim 72, wherein the parameters are encrypted using a public key of the server, according to the described encoding scheme.

Claim 74 (previously presented): The system according to Claim 72, wherein the first security information comprises a client nonce and the second security information comprises a server nonce.

Claim 75 (currently amended): A computer program product for securely establishing a connection between a client application and a server application, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for sending, from the client application to the server application, a first message that uses a first pre-existing message type, wherein the first message requests information from the server application and includes a parameter portion, the parameter portion containing zero or more parameters that may be used by the server application in creating the requested information;

computer-readable program code means for selecting, by the server application responsive to receiving the first message, a message encoding scheme without using information from, or pre-arranged with, the client application;

computer-readable program code means for using, by the server application, the selected message encoding scheme to encrypt the requested information that responds to the first message, the requested information created using zero or more of the zero or more parameters; and

computer-readable program code means for sending, from the server application to the client application, a second message, responsive to receiving the first message, wherein:

the second message uses a second pre-existing message type;

the second message contains the encrypted requested information; and

the second message has security information piggy-backed thereon, the piggy-backed security information enabling the client application to determine the selected message encoding scheme, such that the client application can then decrypt the encrypted requested information ~~, which has been created using zero or more of the zero or more parameters and which has been encrypted using a session key;~~

~~the session key has been created using a server nonce; and~~

~~the second message further contains the server nonce, encrypted using a public key of the client application~~.

Claim 76 (currently amended): The computer program product according to Claim 75, wherein a client-provided ~~client~~ nonce is ~~also used when creating the session key, and wherein the client nonce is~~ transmitted on the first message and is used with a server-provided nonce to create a session key for input to the selected message encoding scheme in the computer-readable program code means for using.

Claim 77 (previously presented): A computer program product for securely establishing a connection between a client application and a server application, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for sending, from the client application to the server application, a first message that uses a first pre-existing message type, wherein the first message requests information from the server application and signals the server application to propose an encoding scheme to be used for securely establishing the connection;

computer-readable program code means for sending, from the server application to the client application, a second message in response to the first message, wherein the second message uses a second pre-existing message type and requests the client application to re-send the information request from the first message, and wherein the second message also transmits a description of the encoding scheme proposed by the server application;

computer-readable program code means for sending, from the client application to the server application, a third message in response to the second message, wherein the third message uses the first pre-existing message type and re-sends the information request from the first message, along with zero or more parameters to be used by the server application in creating the requested information and first security information for use by the server application in securely establishing the connection, according to the described encoding scheme; and

computer-readable program code means for sending, from the server application to the client application, a fourth message in response to the third message, wherein the fourth message uses a third pre-existing message type and contains the requested information, which has been encrypted using a session key created using the first security information as an input, and wherein the fourth message further comprises second security information which was also used as an input when creating the session key, the second security information encrypted such that it can be decrypted only by the client application.

Claim 78 (previously presented): The computer program product according to Claim 77, wherein the parameters are encrypted using a public key of the server, according to the described encoding scheme.

Claim 79 (previously presented): The computer program product according to Claim 77, wherein the first security information comprises a client nonce and the second security information comprises a server nonce.